2002P14781

B2

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04L 9/08 — A1

(11) Internationale Veröffentlichungsnummer: **WO 98/02991**

(43) Internationales Veröffentlichungsdatum: 22. Januar 1998 (22.01.98)

(21) Internationales Aktenzeichen: PCT/EP96/03061

(22) Internationales Anmeldedatum: 12. Juli 1996 (12.07.96)

(71)(72) Anmelder und Erfinder: SENG, Ulrich [DE/DE]; Bäckergasse 17, D-82335 Berg (DE).

(74) Anwalt: SCHOPPE, Fritz; P.O. Box 71 08 67, D-81458 München (DE).

(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO Patent (KE, LS, MW, SD, SZ, UG), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: KEY DISTRIBUTION PROCESS BETWEEN TWO UNITS IN AN ISDN/INTERNET CONNECTION

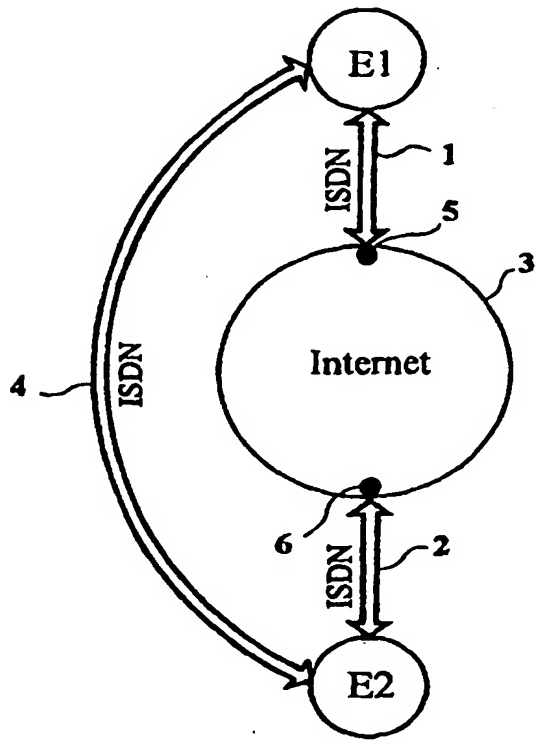
(54) Bezeichnung: VERFAHREN ZUR SCHLÜSSELVERTEILUNG ZWISCHEN ZWEI EINHEITEN IN EINER ISDN/INTERNET VERBINDUNG

(57) Abstract

A process is disclosed for requesting and transmitting confidential information, in particular a key, from a second unit to a first unit during a connection of the first unit to the second unit through an ISDN connection and the internet. The process has the following steps: a connection is established between the first unit and the second unit through the ISDN B-channel and the internet; the call number of the first unit and a request for confidential information, in particular a key request, are transmitted to the second unit; the confidential information is transmitted by the second unit through the ISDN D-channel; and a connection is established through the ISDN B-channel between the second unit and the first unit, in case the B-channel is free, to acknowledge the transmission of confidential information.

(57) Zusammenfassung

Ein Verfahren ermöglicht das Anfordern und Übertragen einer vertraulichen Information, insbesondere eines Schlüssels, von einer zweiten Einheit zu einer ersten Einheit während einer bestehenden Verbindung der ersten Einheit über eine ISDN-Verbindung und das Internet zu der zweiten Einheit durch folgende Verfahrensschritte: Aufbauen einer Verbindung zwischen der ersten Einheit über den B-Kanal des ISDN und über das Internet zu der zweiten Einheit; Übertragen der Rufnummer der ersten Einheit und einer Anforderung einer vertraulichen Information, insbesondere Schlüsselanforderung, an die zweite Einheit; Übertragen der vertraulichen Information von der zweiten Einheit über den D-Kanal des ISDN; und Aufbauen einer Verbindung über den B-Kanal des ISDN zwischen der zweiten Einheit und der ersten Einheit, falls der B-Kanal frei ist, um die Übertragung der vertraulichen Information zu quittieren.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

SDOCID: <WO___9802991A1_I_>

VERFAHREN ZUR SCHLÜSSELVERTEILUNG ZWISCHEN ZWEI EINHEITEN IN EINER ISDN/INTERNET VERBINDUNG

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zum Anfordern und Übertragen einer vertraulichen Information, insbesondere eines Schlüssels zum Verschlüsseln oder Entschlüsseln von Daten. Insbesondere befaßt sich die vorliegende Erfindung mit einem Verfahren zum Anfordern und Übertragen eines Schlüssels zum Verschlüsseln oder Entschlüsseln von Daten von einer zweiten Einheit zu einer ersten Einheit während einer bestehenden Verbindung von der ersten Einheit über ein verbindungsorientiertes Datennetz, das einen Signalisierungskanal und einen Nachrichten-/Datenkanal hat und ein verteiltes, nicht-verbindungsorientiertes Datennetz, zu der zweiten Einheit. In einer besonderen Ausgestaltung betrifft die Erfindung die Anwendung dieses Verfahrens auf das sogenannte Telebanking.

Es ist insbesondere aufgrund des weit verbreiteten Einsatzes von Datennetzen, insbesondere des sogenannten Internet üblich geworden, Daten bei Datenlieferanten, nämlich beispielsweise Datenbanken oder anderen datenliefernden Stellen über derartige Datennetze zu bestellen, woraufhin die Datenbanken bzw. datenliefernden Stellen dem Anwender, der einen Datensatz bestellt, typischerweise zunächst einen Schlüssel über das Datennetz übertragen, woraufhin der gewünschte Datensatz in verschlüsselter Form über das verteilte Datennetz übertragen wird, damit der Anwender nach Empfang des verschlüsselten Datensatzes diesen entschlüsseln und für seine Zwecke verwenden kann. Wenn man sich zum Zwecke der Lieferung von Daten des Internet bedient, welches ein verteil-

tes, nicht-verbindungsorientiertes Datennetz ist, so sind die über das Internet übertragenen Daten an sich auch weiteren Internetteilnehmern zugänglich, für die die Daten nicht bestimmt sind. Wird nun auch der Schlüssel zum Entschlüsseln von Daten über das Internet übertragen, so kann nicht ausgeschlossen werden, daß unberechtigte Dritte nicht nur die verschlüsselten Datensätze, sondern auch den Schlüssel erhalten.

Aus diesem Grunde werden bei besonders sicherheitsrelevanten Datenübertragungen über das Internet die Schlüssel für das Verschlüsseln oder Entschlüsseln von Daten separat, beispielsweise per Post, an den Anwender übermittelt.

Bei dem sogenannten Telebanking, bei dem der Schlüssel der Bank als Nachweis der Zugriffsberechtigung eines Bankkunden auf bestimmte Bankdienstleistungen, wie beispielsweise die Durchführung von Überweisungen, dient, wird das erörterte Sicherheitsproblem dadurch bewältigt, daß die Bank dem Anwender beispielsweise zehn Schlüssel zuteilt und ihm per Post übermittelt, mit denen er zehn Überweisungen veranlassen kann. Für jede Überweisung, die der Anwender über das Internet bei seiner Bank veranlaßt, verbraucht er einen der ihm überlassenen Schlüssel, so daß es erforderlich ist, nach dem Verbrauch der beispielsweise zehn überlassenen Schlüssel zehn neue Schlüssel anzufordern, die von der Bank an den Anwender übersandt werden. Dieses Verfahren ist nicht nur mühselig und langsam, sondern auch sicherheitstechnisch nicht ganz unproblematisch, falls der von der Bank an den Kunden übersandte Brief mit den jeweils neuen Schlüsseln in unberechtigte Hände gerät.

Bei dem beschriebenen Anwendungsfall von Datenbestellungen ist es für den Anwender gleichfalls mühselig, im Falle von geheimzuhaltenden, wichtigen Datensätzen zunächst auf eine separate Übermittlung eines Schlüssels zur Entschlüsselung der an ihn übertragenen verschlüsselten Datensätze warten zu müssen. Falls jedoch zum Zwecke der erleichterten Abwicklung

auch der Schlüssel über das Internet übertragen wird, bestehen die genannten Datensicherheitsprobleme.

Wie an sich allgemein bekannt ist, findet ein Zugriff eines Anwenders auf das Internet nicht direkt statt, sondern unter Zwischenschaltung eines verbindungsorientierten Datennetzes, wie beispielsweise des ISDN-Netzes, welches den Anwender mit einem Knoten des Internet verbindet, wobei typischerweise wiederum das Internet an einem anderen Knoten über ein weiteres verbindungsorientiertes Datennetz, wie beispielsweise ebenfalls das ISDN-Netz, mit einer datenliefernden Stelle, wie beispielsweise einer Bank, einer Datenbank oder ähnlichem, verbunden ist.

Ausgehend von diesem Stand der Technik liegt der vorliegenden Erfindung somit die Aufgabe zugrunde, ein Verfahren zum Anfordern einer vertraulichen Information und zum Übertragen derselben von einer zweiten Einheit zu einer ersten Einheit während einer bestehenden Verbindung von der ersten Einheit über ein verbindungsorientiertes Datennetz und ein verteiltes Datennetz zu der zweiten Einheit zu schaffen.

Diese Aufgabe wird durch ein Verfahren gemäß Anspruch 1 gelöst.

Die Erfindung schafft ein Verfahren zum Anfordern einer vertraulichen Information und zum Übertragen derselben von einer zweiten Einheit zu einer ersten Einheit während einer bestehenden Verbindung von der ersten Einheit über ein verbindungsorientiertes Datennetz, das einen Signalisierungskanal und einen Nachrichten-/Datenkanal aufweist, und ein verteiltes, nicht-verbindungsorientiertes Datennetz zu der zweiten Einheit, mit folgenden Schritten:

- Aufbauen einer Verbindung zwischen der ersten Einheit über den Nachrichten-/Datenkanal des verbindungsorientierten Datennetzes und über das verteilte

nicht-verbindungsorientierte Datennetz zu der zweiten Einheit;

- Übertragen der Rufnummer der ersten Einheit und einer Anforderung bezüglich der vertraulichen Information an die zweite Einheit;

- Übertragen der vertraulichen Information von der zweiten Einheit über den Signalisierungskanal des verbindungsorientierten Datennetzes zu der ersten Einheit; und

- falls der Nachrichten-/Datenkanal des verbindungsorientierten Datennetzes zwischen der zweiten Einheit und der ersten Einheit frei ist, Aufbauen einer Verbindung zwischen der zweiten Einheit und der ersten Einheit.

Bei dem erfindungsgemäßen Verfahren wird also zunächst eine Verbindung zwischen der ersten Einheit über den Nachrichten-/Datenkanal des verbindungsorientierten Datennetzes, nämlich vorzugsweise des ISDN-Netzes, und über das verteilte, nicht-verbindungsorientierte Datennetz, nämlich vorzugsweise das Internet, zu der zweiten Einheit geschaffen. Dieser erste Schritt ist im Zusammenhang mit der Nutzung des Internets an sich üblich.

Während der bestehenden Verbindung zwischen der ersten Einheit und der zweiten Einheit überträgt die erste Einheit ihre Rufnummer sowie Anforderung einer vertraulichen Information, insbesondere eine Schlüsselanforderung, an die zweite Einheit. Sodann überträgt die zweite Einheit die vertrauliche Information über den Signalisierungskanal des verbindungsorientierten Datennetzes, nämlich den D-Kanal im Falle des ISDN-Netzes, zu der ersten Einheit. Falls der Nachrichten-/Datenkanal des verbindungsorientierten Datennetzes zwischen der zweiten Einheit und der ersten Einheit frei ist, wird nunmehr ein Verbindungsaufbau über den Nach-

richten-/Datenkanal bzw. B-Kanal im Falle des ISDN-Netzes vorgenommen, woraufhin vorzugsweise eine Quittierung über den Nachrichten-/Datenkanal zur Bestätigung des empfangenen Schlüssels vorgenommen wird, bevor die Verbindung abgebaut wird.

Im Falle des IDSN-Netzes macht sich die Erfindung die besondere Fähigkeit des IDSN-Protokolls hinsichtlich der Signalisierung zu Nutze, nämlich die Möglichkeit der Signalisierung von Nachrichten zwischen den Teilnehmern unter Verwendung des UUS-Frame auch während einer bestehenden Verbindung eines der Teilnehmer mit einer dritten Partei, also im vorliegenden Fall während einer bestehenden Verbindung der ersten Einheit über den Nachrichten-/Datenkanal mit einem Knoten des Internet.

Ein bevorzugtes Ausführungsbeispiel des erfindungsgemäßen Verfahrens wird nachfolgend unter Bezugnahme auf die beiliegenden Figuren näher erläutert. Es zeigen:

Fig. 1a bis 1c ein Flußdiagramm eines Ausführungsbeispiels des erfindungsgemäßen Verfahrens zum Anfordern und Übertragen einer vertraulichen Information; und

Fig. 2 eine schematische Darstellung der Verbindungen, die durch das erfindungsgemäße Verfahren aufgebaut werden.

Bevor auf das bevorzugte Ausführungsbeispiel gemäß Fig. 1 im einzelnen Bezug genommen wird, sei hervorgehoben, daß unter den Begriffen "vertrauliche Information bzw. Schlüssel" im Sinne der vorliegenden Anmeldung jegliche sicherheitsrelevante Daten zu verstehen sind, sei es, daß diese beispielsweise zum Verschlüsseln von Daten, beispielsweise zum Entschlüsseln von Daten oder beispielsweise für das Steuern oder den Nachweis einer Zugangs- oder Zugriffsberechtigung dienen.

Das nunmehr zu erläuternde Ausführungsbeispiel betrifft eine Datenverbindung zwischen zwei Teilnehmern, die als erste und zweite Einheit bezeichnet werden über ISDN und das Internet. Anstelle des ISDN kommt jedoch jedes verbindungsorientierte Datennetz in Betracht. Anstelle des Internet kommt jedes verteilte, nicht-verbindungsorientierte Datennetz in Betracht.

Das Verfahren geht in dem ersten Verfahrensschritt S1 von einer bei Nutzung des Internets stehenden Verbindung über den Nachrichten-/Datenkanal bzw. B-Kanal des ISDN zwischen einer ersten Einheit E1 und dem Internet 3 aus. Bei dem hier zu beschreibenden Ausführungsbeispiel besteht eine Datenverbindung über den B-Kanal eines Datenweges 1 des ISDN-Netzes zwischen der ersten Einheit E1 und einem Knoten 5 des Internet, der den Zugang für die erste Einheit E1 in das Internet 3 bildet. Die zweite Einheit E2 steht entweder direkt mit dem Internet 3 in Verbindung oder, wie dies bei dem hier gezeigten Ausführungsbeispiel der Fall ist, über einen weiteren Datenweg 2 des ISDN, der eine Verbindung der zweiten Einheit E2 mit einem weiteren Knoten 6 darstellt.

Aus Gründen der Anschaulichkeit sei zunächst davon ausgegangen, daß es sich bei der ersten Einheit E1 um einen Anwender und bei der zweiten Einheit E2 um eine datenliefernde Stelle, wie beispielsweise eine Datenbank, eine Bank mit Telebanking-Dienstleistungen oder dergleichen handelt.

Um von der zweiten Einheit einen Schlüssel beispielsweise zur Entschlüsselung von Datensätzen oder zum Nachweis einer Zugriffsberechtigung für Bankdienstleistungen oder andere sicherheitsrelevante Daten zu erhalten, sendet die erste Einheit E2 bei dem zweiten Verfahrensschritt S2 ihre Rufnummer, welche im Fall des ISDN auch als "calling party number" bekannt ist, gegebenenfalls zusammen mit einer Geheimnummer bzw. PIN-Nummer über die beschriebene Verbindung an die zweite Einheit zusammen mit einer Anforderung eines

Schlüssels.

Nach Erhalt der Rufnummer und gegebenenfalls der PIN-Nummer prüft die zweite Einheit bei dem dritten Schritt S3, ob die Rufnummer eine einer Mehrzahl von vorab gespeicherten Teilnehmerrufnummern ist. Wenn es sich bei der zweiten Einheit um eine Datenbank handelt, kann bei dieser Prüfung ermittelt werden, ob die Rufnummer diejenige eines Datenbankkunden ist, der bei der betreffenden Datenbank Daten abfragen darf und anhand der Rufnummer sowie gegebenenfalls weiterer Daten, wie beispielsweise dem Namen und/oder der PIN-Nummer registriert ist. Im Falle der Bank überprüft die die zweite Einheit E2 bildende Bank, ob die Rufnummer der anrufenden ersten Einheit die registrierte Rufnummer eines Kunden ist, und überprüft ferner die Übereinstimmung der Rufnummer mit weiteren übermittelten Daten, wie beispielsweise der PIN-Nummer, dem Kundennamen und dergleichen. Wird bei diesem Prüfschritt S3 festgestellt, daß die Rufnummer und gegebenenfalls PIN-Nummer sowie die genannten weiteren Daten entweder nicht registriert oder nicht korrekt sind, also nicht als zusammengehörig abgespeichert bei der zweiten Einheit vorliegen, so wird bei dem Schritt S4 der Ruf abgewiesen bzw. der Verbindungsaufbauversuch abgebrochen und gegebenenfalls eine Fehlermeldung erzeugt.

Falls die Rufnummer und die genannten möglichen weiteren Daten registriert sind und sich bei dem Prüfschritt S3 als korrekt erweisen, fährt das Verfahren mit dem Schritt S5 fort, bei dem eine vertrauliche Information beispielsweise in Form eines Schlüssels erzeugt wird.

Bei dem sechsten Verfahrensschritt kopiert die zweite Einheit E2 die vertrauliche Information beispielsweise in Form des Schlüssels in den sogenannten UUS-Frame des Signalisierungskanals bzw. des D-Kanals bei ISDN. Bei dem siebten Schritt S7 überträgt die zweite Einheit die im UUS-Frame aufgebauten Informationen über den Signalisierungskanal bzw. D-Kanal bei ISDN an die im Schritt S2 gesendete Rufnummer

(calling party number) der ersten Einheit, also des Anwenders. Es sei hervorgehoben, daß es aufgrund der verbindungsorientierten Natur des ISDN seitens des Anwenders nicht möglich ist, Manipulationen hinsichlich seiner angegebenen Rufnummer vorzunehmen, da anderenfalls ihn der gewünschte Schlüssel bei der Schlüsselübertragung im siebten Verfahrensschritt S7 nicht erreichen würde.

Bei dem folgenden Verfahrensschritt S8 prüft das Verfahren, ob die Quittierung über den Erhalt der vertraulichen Information beispielsweise in Form des Schlüssels gleichzeitig mit dem Rücksenden einer Rückinformation an den Lieferanten bzw. die zweite Einheit E2 erfolgen soll. Falls dies der Fall ist, fährt das Verfahren mit dem Verfahrensschritt S12 fort.

Anderenfalls wird bei dem Schritt S9 überprüft, ob der Nachrichten-/Datenkanal bzw. B-Kanal der ISDN-Verbindung zwischen den beiden Einheiten E1 und E2 frei ist. Falls dies der Fall ist, fährt das Verfahren mit dem Schritt S10 fort, bei dem ein Verbindungsaufbau des Nachrichten-/Datenkanals bzw. B-Kanals im Falle eines ISDN-Netzwerkes vorgenommen wird.

Bei dem Schritt S11 erzeugt die erste Einheit eine Quittung für den Erhalt der vertraulichen Information bzw. des Schlüssels und sendet diese über den Signalisierungskanal bzw. D-Kanal bei ISDN an die zweite Einheit E2, bevor eine Signalisierung zum Auftrennen der Verbindung (die Prozedur "release complete" bei ISDN) über den Signalisierungskanal vorgenommen wird. Hiernach fährt das Verfahren mit dem Schritt S16 fort.

Falls die Überprüfung bei dem Schritt S8 ergibt, daß das Rücksenden einer Rückinformation bei der Quittierung des Erhalts der vertraulichen Information erwünscht ist, fährt das Verfahren mit dem Schritt S12 fort, bei dem die Rückinformation, die beim Beispielsfall des Telebankings die

Kreditkartennummer oder eine Kontoinformation sein kann, von der ersten Einheit E1 in den UUS-Frame des Kommandos zum Auftrennen der Signalisierung des Signalisierungskanals (die Prozedur "release complete" für die Übertragung im D-Kanal bei ISDN) kopiert wird.

Die folgenden Schritte S13, S14, S15 entsprechen mit der Ausnahme den Schritten S9, S10 und S11, daß beim Schritt S15 im Gegensatz zum Schritt S11 bei der Signalisierung zum Auftrennen der Verbindung (Prozedure "release complete" bei ISDN) die im UUS-Frame aufgebaute Rückinformation an den Lieferanten bzw. die zweite Einheit E2 übertragen wird. Die Auswertung der Rückinformation durch die zweite Einheit E2 ist im Flußdiagramm nicht im Einzelnen beschrieben, da sie von dem jeweiligen Anwendungsfall abhängt. Beispielsweise kann im Fall des Telebanking die Bank, die vom Kunden erhaltene Rückinformation beispielsweise in Form einer Kreditkartennummer zusammen mit den gewünschten Buchungsvorgängen abspeichern, um eine weitere Erhöhung der Sicherheit des Telebankingverfahrens zu erreichen.

Bei dem abschließenden Schritt S16 übernimmt die erste Einheit E1 bzw. der Anwender die vertrauliche Information beispielsweise in Form des Schlüssels, welcher über den Signalisierungskanal übertragen worden ist.

Es sei hervorgehoben, daß das soeben beschriebene Verfahren zwar die Übertragung des Schlüssels von der zweiten Einheit über den Signalisierungskanal an die erste Einheit vornimmt, jedoch grundsätzlich darauf abstellt, einen Verbindungsaufbau über den Nachrichten-/Datenkanal dies ISDN-Netzes zwischen der zweiten Einheit und der ersten Einheit herbeizuführen, falls der Nachrichten-/Datenkanal frei ist. Im Gegensatz zu Datenübertragungsverfahren, die allein auf eine Datenübermittlung über den Signalisierungskanal ohne beabsichtigten Verbindungsaufbau abstellen, ist daher das beschriebene Verfahren postalisch zulässig.

Anhand des Flußdiagrammes gemäß Fig. 1 wurde nicht weiter erläutert, welche Aktionen nach Übertragung der vertraulichen Information bzw. des Schlüssels durchgeführt werden, da die weiteren Zugriffe der ersten Einheit auf die zweite Einheit unter Nutzung der vertraulichen Information bzw. des Schlüssels an sich dem Stand der Technik bekannt sind. Bei dem Beispielsfall, bei dem es sich bei der zweiten Einheit um eine Datenbank handelt und es sich bei der ersten Einheit um einen Anwender handelt, der von der Datenbank Datensätze übermittelt haben möchte, kann nun die Übertragung der vom Anwender gewünschten, verschlüsselten Datensätze über das Internet vorgenommen werden, welche sodann vom Anwender entschlüsselbar sind.

Im beschriebenen Beispielsfall des Telebanking kann nunmehr der Anwender, also die erste Einheit auf die Bank, also die zweite Einheit, zugreifen und jeweils unter Nutzung der übermittelten Schlüssel Bankvorgänge auslösen, also beispielsweise Überweisungen tätigen.

Patentansprüche

1. Verfahren zum Anfordern einer vertraulichen Information und zum Übertragen derselben von einer zweiten Einheit zu einer ersten Einheit während einer bestehenden Verbindung von der ersten Einheit über ein verbindungsorientiertes Datennetz, das einen Signalisierungskanal und einen Nachrichten-/Datenkanal aufweist, und ein verteiltes, nicht-verbindungsorientiertes Datennetz zu der zweiten Einheit, mit folgenden Schritten:

   - Aufbauen (S1) einer Verbindung zwischen der ersten Einheit (E1) über den Nachrichten-/Datenkanal des verbindungsorientierten Datennetzes (1,2,4) und über das verteilte nicht-verbindungsorientierte Datennetz (3) zu der zweiten Einheit (E2);

   - Übertragen (S2) der Rufnummer der ersten Einheit (E1) und einer Anforderung bezüglich der vertraulichen Information an die zweite Einheit (E2);

   - Übertragen (S7) der vertraulichen Information von der zweiten Einheit (E2) über den Signalisierungskanal des verbindungsorientierten Datennetzes (1,2,4) zu der ersten Einheit (E1); und

   - falls der Nachrichten-/Datenkanal des verbindungsorientierten Datennetzes zwischen der zweiten Einheit (E2) und der ersten Einheit (E1) frei ist, Aufbauen einer Verbindung (S10, S14) zwischen der zweiten Einheit (E2) und der ersten Einheit (E1).

2. Verfahren nach Anspruch 1, bei dem

   - das verbindungsorientierte Datennetz das ISDN-Netz ist;

- der Nachrichten-/Datenkanal der B-Kanal ist; und

- der Signalisierungskanal der D-Kanal ist.

3. Verfahren nach Anspruch 1 oder 2, bei dem das verteilte, nicht-verbindungsorientierte Datennetz das Internet ist.

4. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der Schritt des Übertragens (S2) der Rufnummer ferner das Übertragen einer PIN-Nummer umfaßt.

5. Verfahren nach einem der vorhergehenden Ansprüche, ferner mit dem Schritt des Prüfens (S3), ob die bei dem Schritt (S2) des Übertragens der Rufnummer der ersten Einheit übertragene Rufnummer eine registrierte Rufnummer ist; und

falls die Überprüfungs (S3) ein negatives Ergebnis liefert, Durchführen (S4) einer Fehlermeldung und/oder eines Abbruchs der Verbindung.

6. Verfahren nach einem der vorhergehenden Ansprüche, mit folgenden Schritten vor dem Schritt (S7) des Übertragens der vertraulichen Information:

- Erzeugen (S5) der vertraulichen Information;

- Kopieren (S6) der vertraulichen Information in den UUS-Frame des D-Kanals; und

- Übertragen (S7) der im UUS-Frame aufgebauten Information über den D-Kanal des ISDN an die Rufnummer der ersten Einheit.

7. Verfahren nach einem der vorhergehenden Ansprüche, mit folgenden weiteren Schritte nach dem Schritt (S7) des Übertragens der vertraulichen Information:

- Prüfen (S8), ob eine Rückinformation von der ersten Einheit (E1) an die zweite Einheit (E2) übertragen werden soll; und

- falls dies der Fall ist, Übertragen (S15) der Rückinformation von der ersten Einheit (E1) an die zweite Einheit (E2) über den Signalisierungskanal des verbindungorientierten Datennetzes.

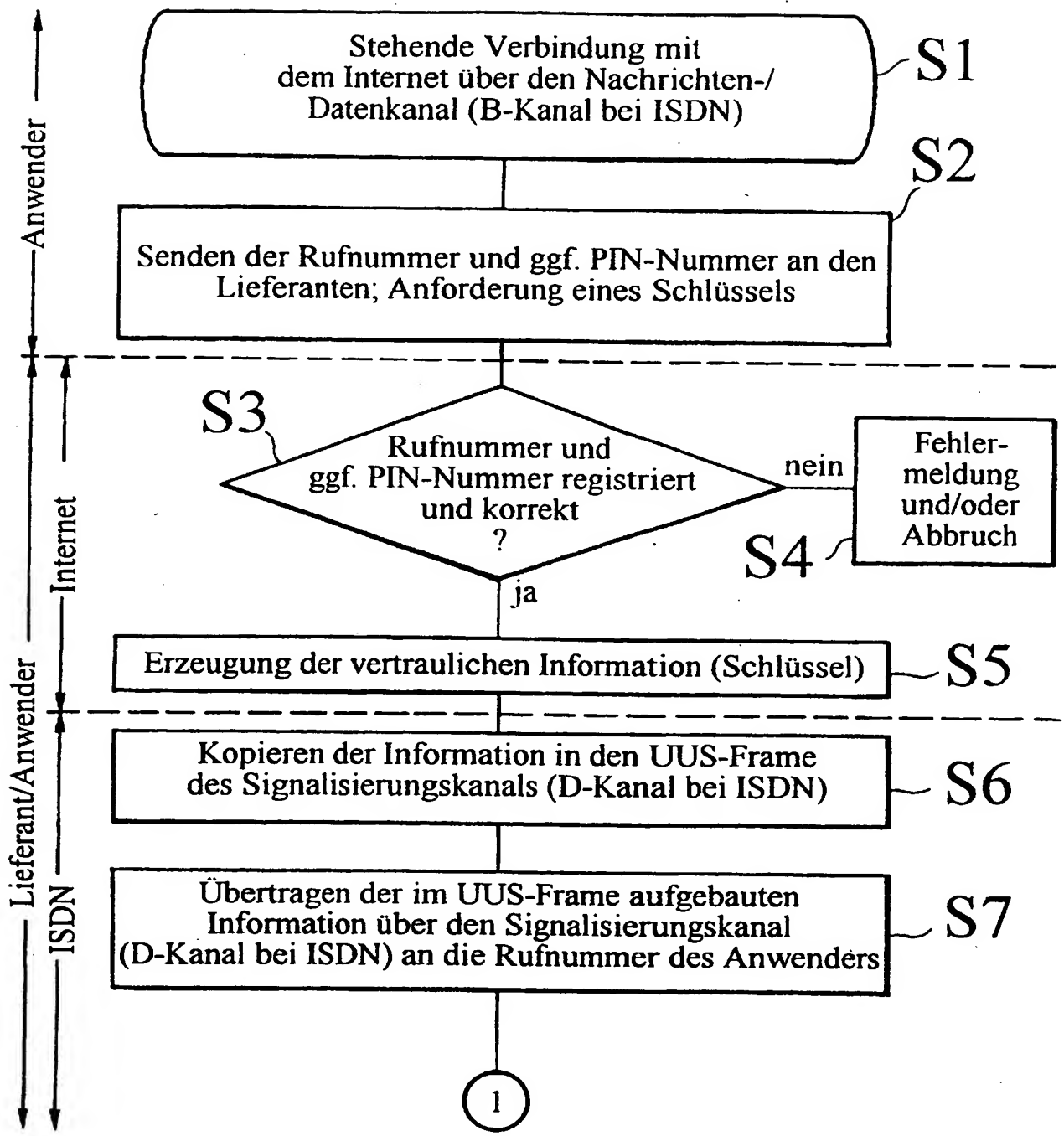


Fig.1a

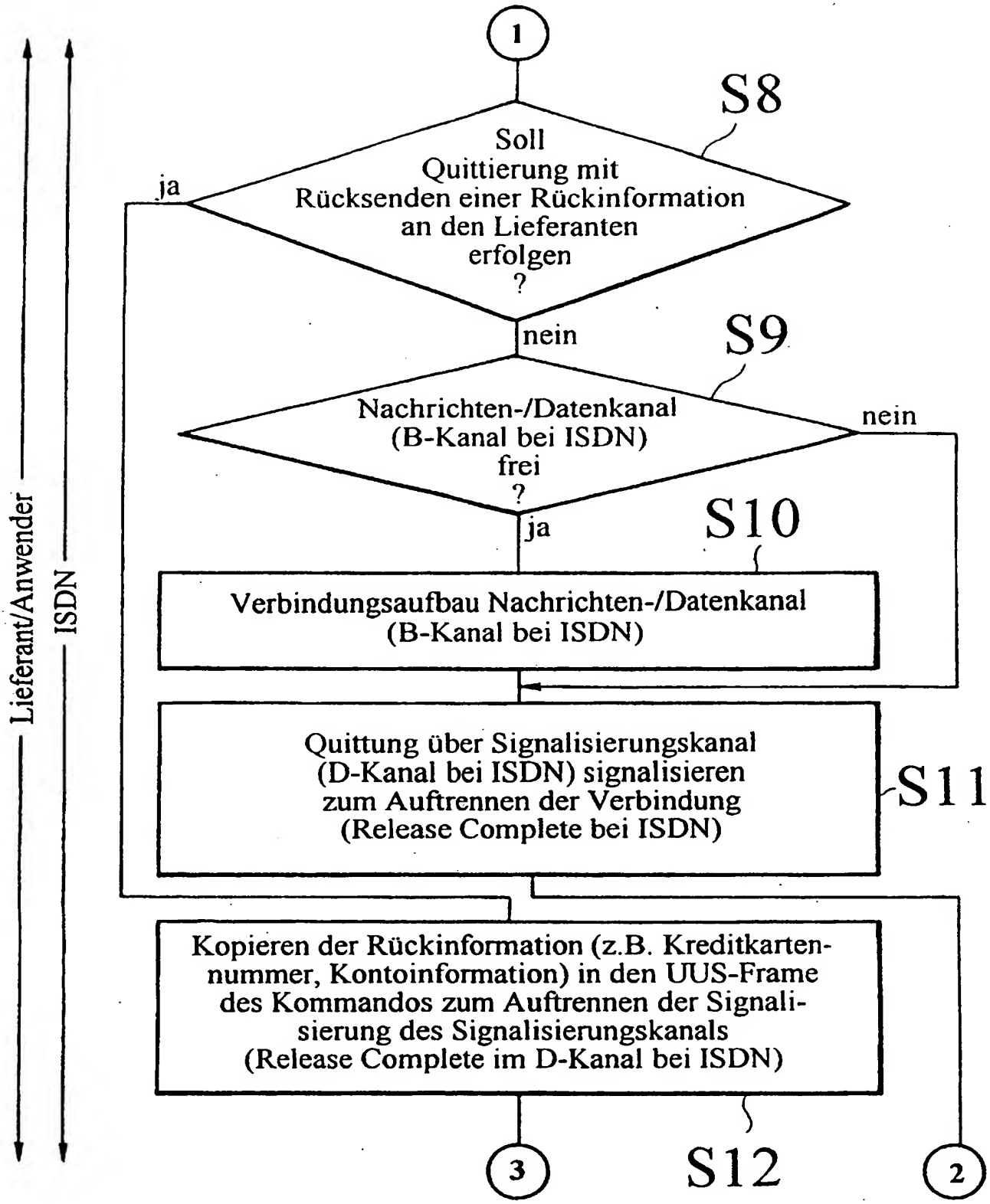


Fig.1b

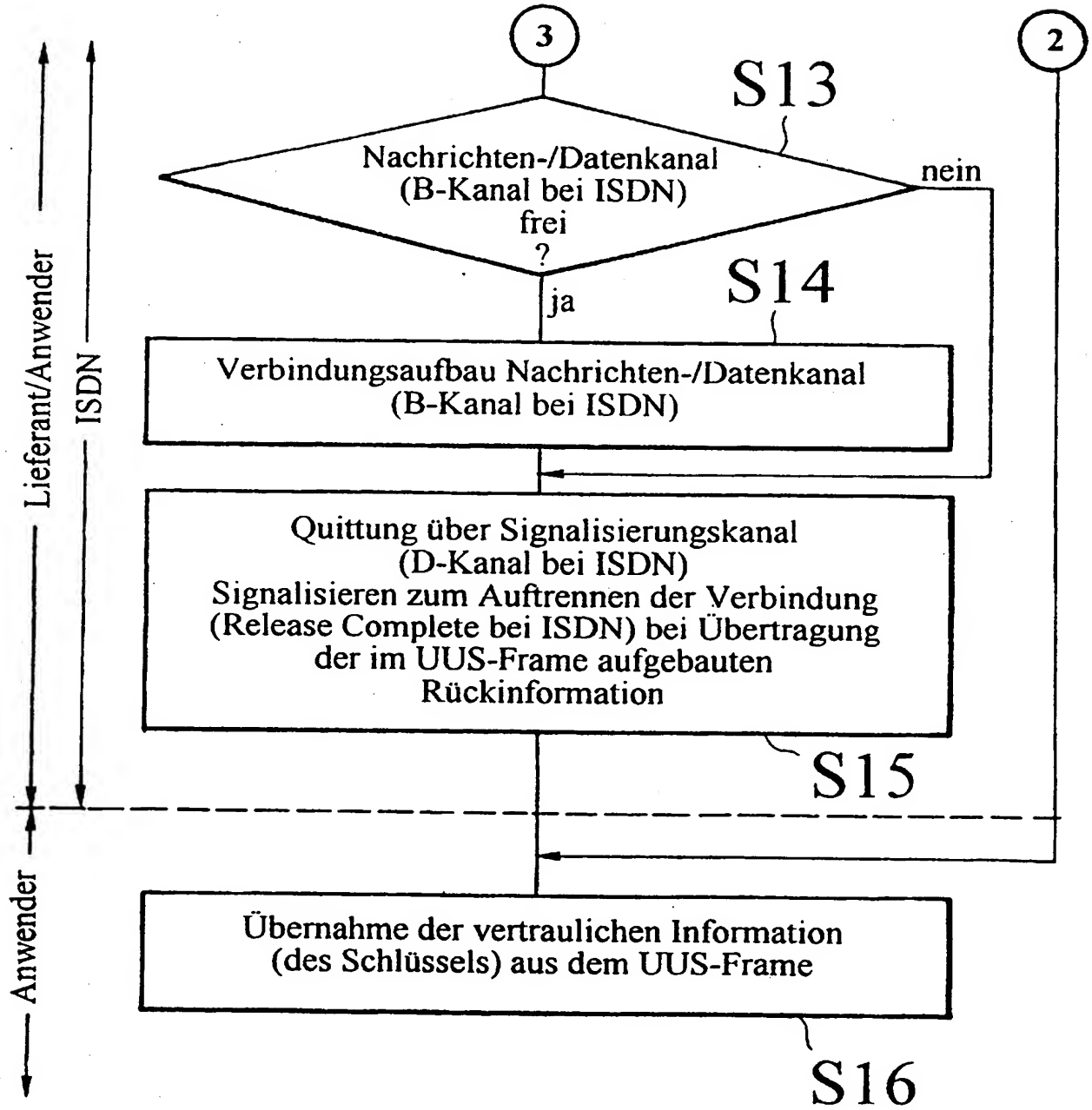


Fig.1c

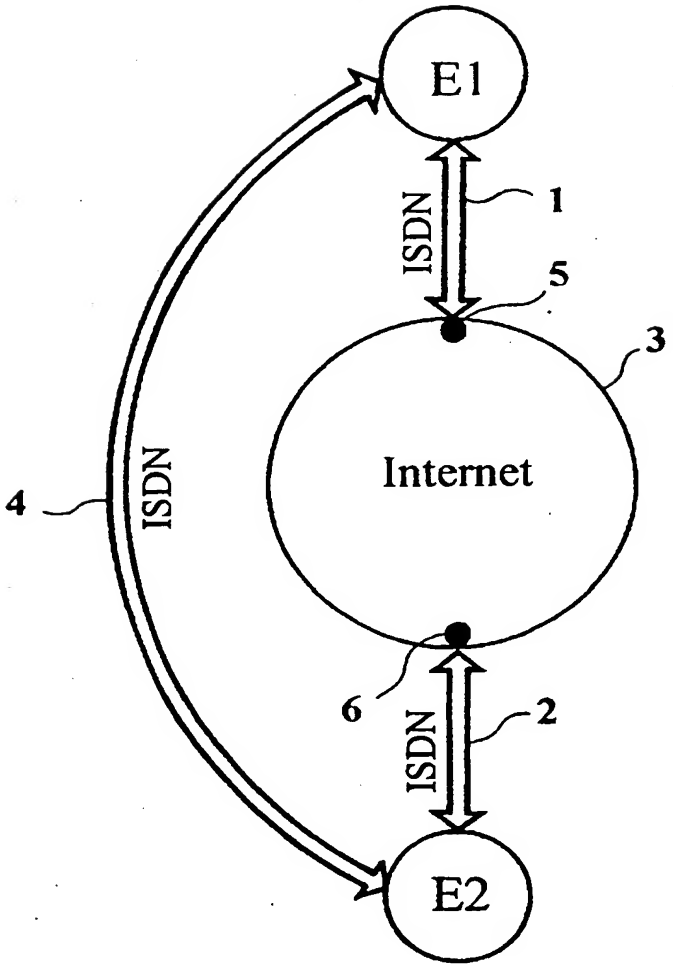


Fig.2

INTERNATIONAL SEARCH REPORT

Internat ' Application No
PCT/EP 96/03061

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	COMSIG 88. SOUTHERN AFRICAN CONFERENCE ON COMMUNICATIONS AND SIGNAL PROCESSING. PROCEEDINGS. (IEEE CAT. NO.88TH0219-6), PRETORIA, SOUTH AFRICA, 24 JUNE 1988, ISBN 0-87942-709-4, 1988, NEW YORK, NY, USA, IEEE, USA, pages 165-170, XP002028403 CLAASSEN G J ET AL: "Secure communication procedure for ISDN" see page 166, right-hand column, line 36 - line 72 see page 169, left-hand column, line 20 - page 170, left-hand column, line 32 see page 170, right-hand column, line 10 - line 20 see figure 7 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
27 March 1997	22.04.97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Lydon, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna[illegible] Application No
PCT/EP 96/03061

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, PROCEEDINGS OF INTERNET SOCIETY SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEMS SECURITY, SAN DIEGO, CA, USA, 22-23 FEB. 1996, ISBN 0-8186-7222-6, 1996, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC. PRESS, USA, pages 114-127, XP002028404 KRAWCZYK H: "SKEME: a versatile secure key exchange mechanism for Internet" see abstract see page 120, right-hand column, line 9 - line 38 ---	1
A	EP 0 693 836 A (SUN MICROSYSTEMS) 24 January 1996 see page 7, line 12 - page 8, line 40 see figure 2 -----	1

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internal Application No
PCT/EP 96/03061

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 693836 A	24-01-96	US 5588060 A	24-12-96
		US 5416842 A	16-05-95
		JP 8008895 A	12-01-96

INTERNATIONALER RECHERCHENBERICHT

Interna·les Aktenzeichen
PCT/EP 96/03061

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	COMSIG 88. SOUTHERN AFRICAN CONFERENCE ON COMMUNICATIONS AND SIGNAL PROCESSING. PROCEEDINGS. (IEEE CAT. NO.88TH0219-6), PRETORIA, SOUTH AFRICA, 24 JUNE 1988, ISBN 0-87942-709-4, 1988, NEW YORK, NY, USA, IEEE, USA, Seiten 165-170, XP002028403 CLAASSEN G J ET AL: "Secure communication procedure for ISDN" siehe Seite 166, rechte Spalte, Zeile 36 - Zeile 72 siehe Seite 169, linke Spalte, Zeile 20 - Seite 170, linke Spalte, Zeile 32 siehe Seite 170, rechte Spalte, Zeile 10 - Zeile 20 siehe Abbildung 7 --- -/--	1

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
27.März 1997	22.04.97

Name und Postanschrift der Internationale Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Lydon, M

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Interna' 'es Aktenzeichen
PCT/EP 96/03061

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, PROCEEDINGS OF INTERNET SOCIETY SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEMS SECURITY, SAN DIEGO, CA, USA, 22-23 FEB. 1996, ISBN 0-8186-7222-6, 1996, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC. PRESS, USA, Seiten 114-127, XP002028404 KRAWCZYK H: "SKEME: a versatile secure key exchange mechanism for Internet" siehe Zusammenfassung siehe Seite 120, rechte Spalte, Zeile 9 - Zeile 38 ---	1
A	EP 0 693 836 A (SUN MICROSYSTEMS) 24.Januar 1996 siehe Seite 7, Zeile 12 - Seite 8, Zeile 40 siehe Abbildung 2 -----	1

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Interna' 'es Aktenzeichen
PCT/EP 96/03061

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 693836 A	24-01-96	US 5588060 A	24-12-96
		US 5416842 A	16-05-95
		JP 8008895 A	12-01-96